

SyScan^{III}
前瞻資安技術年會

Learn & Fun
In the year 2011, SyScan round of
conferences will kick off in the city-state
of Singapore!



Taiwan, Taipei
台灣·台北

17-18 November 2011

Visualizing the Ghost in the Network: Know the Enemy, and Know Yourself

Benson Wu^{*,†}, Jeremy Chiu[†], Pei-Kan, Anthony Lai[†]

[†] Xecure Lab

^{*} Research Center for Information Technology Innovation, Academia Sinica



Xecure Lab



中央研究院

資訊科技創新研究中心

Research Center for Information Technology Innovation



雲端安全智慧實驗室
Cloud Security Intelligence (CSI) Lab

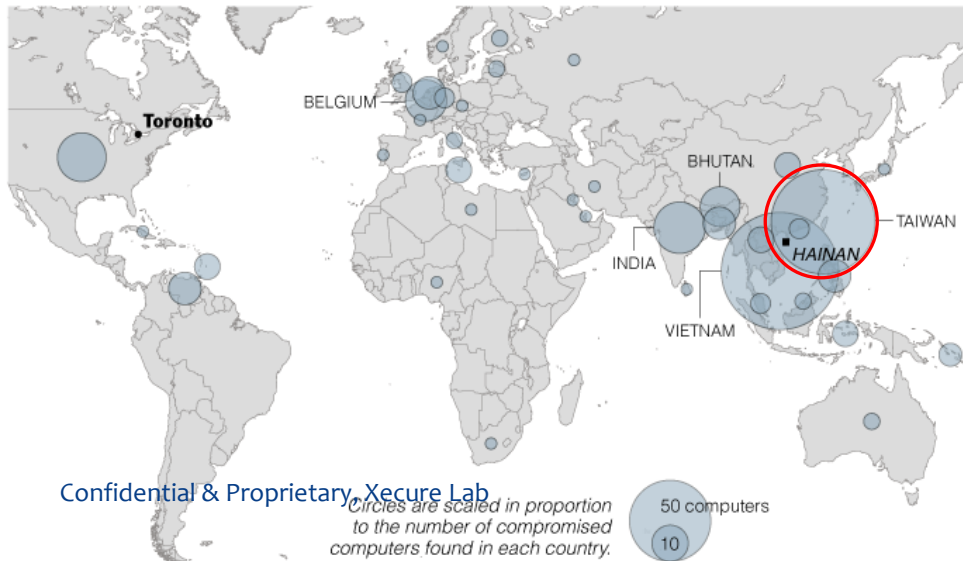
Cyber Espionage Coming?

Taiwan is one of the key battlefields for Cyber Espionage

* GhostNet, Shadows in the Cloud

The Vast Reach of 'GhostNet'

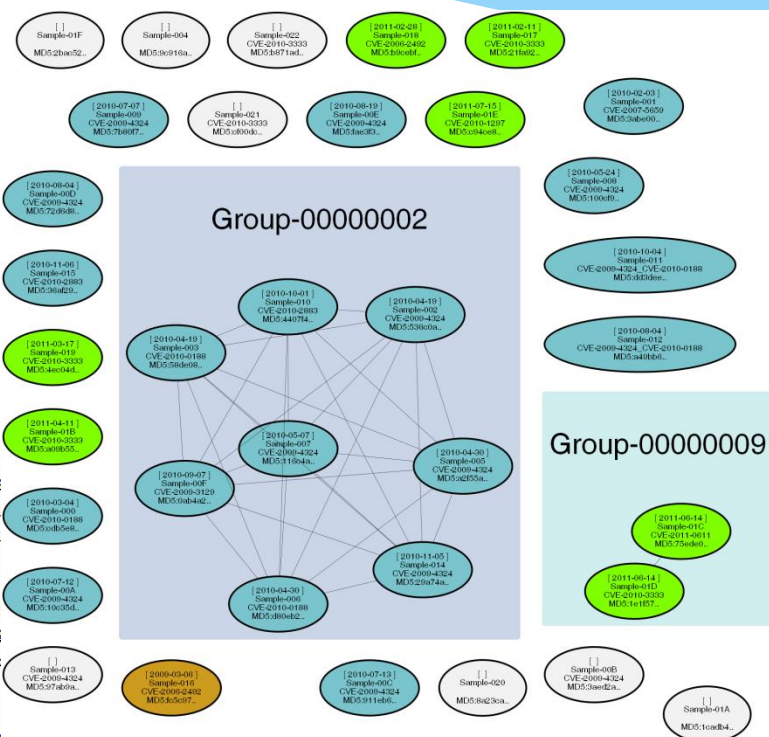
Researchers have detected an intelligence gathering operation involving at least 1,295 compromised computers. Below, the locations of 347 of the compromised machines, many of which were tracked to diplomatic and economic government offices of South and Southeast Asian countries.



Shadows in the Cloud



Academic Sector Suffers from Malicious Emails



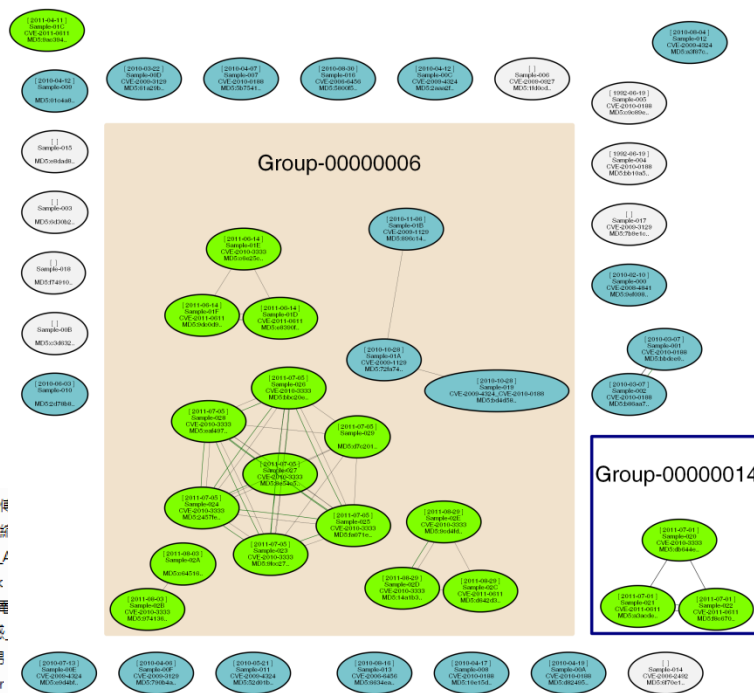
- [2010-03-08] _titx@oa.tku.edu.tw_邀參加兩岸關係研討會_.pdf
- [2010-03-24] _h670928@ndu.edu.tw_2010第十八屆國防管理學術暨實務研討會組建再進 心理健康司的發展_.pdf
- [2010-04-26] _smiles@mail.knu.edu.tw_[研討會]開南大學公共事務管理學
- [2010-04-26] _smiles@mail.knu.edu.tw_[研討會]開南大學公共事務管理學
- [2010-05-03] _zhonggonv@nccu.edu.tw_2010 年中共年報_2010_.doc
- [2010-05-03] _zhonggonv@nccu.edu.tw_2010 年中共年報_2010_.pdf
- [2010-05-06] _jjsung@ntu.edu.tw_蔡政文教授七十華誕系列活動簡報_ATT
- [2010-05-07] _lsf@gate.sinica.edu.tw_201004_遠見民調中心_台灣民意政
- [2010-06-08] _iirj@nccu.edu.tw_天安艦後的朝鮮半島新局勢_ATT77316.p
- [2010-07-07] _ykkao@nccu.edu.tw_關於中共領導人&_35843_查研究.pdf
- [2010-07-11] _iirj@nccu.edu.tw_雙週報_1579期_ATT50892.pdf
- [2010-08-01] _yize.wang01@ndu.edu.tw_港澳每日新聞輯要_(99.08.02).p
- [2010-08-03] _tivx@tku.edu.tw_蘇起：台灣的大三角與小三角_ATT30078.p
- [2010-08-17] _pyang@ntu.edu.tw_美國國防部~解放軍軍力報告_ATT3950
- [2010-08-23] _tasims9@nccu.edu.tw_第二屆「半總統制與民主」學術研討
- [2010-09-07] _wongmh@mail.tku.edu.tw_遠東_9月份全球經濟策略_9.xls
- [2010-09-17] _wongmh@mail.tku.edu.tw_990917覽報_990917.rar
- [2010-10-06] _fen6604@nccu.edu.tw_美國公布共軍軍力報告的重大意義_ATT193278.pd
- [2010-10-22] _sa@gate.sinica.edu.tw_東海大學社會學系：國內中教授演講_ATT25721.pdf
- [2010-10-27] _titx@www2.tku.edu.tw_Fw_11_10研討會議程_Document.pdf
- [2010-10-27] _tivx@tku.edu.tw_11_10研討會議程_Document.pdf

APT File Cluster Graph

Powered by Xecure Lab 2011, <http://www.xecure-lab.com>

- ATT69914.pdf
- 「淡江一甲子行動-全國防軍武大」_ATT96321.pdf
- 師TA及CA補助費用(選錄更正後)_99(1)TA-RA-.rar
- 組織再造 心理健康司的發展_.pdf
- 臨新年快樂_倂.doc
- 本校2011年「春之懷裏」活動_2011.doc
- 四十週年 座談會邀請函_ATT19907.doc
- 38713.rar
- 看一書終生受益.doc_ATT52977.doc
- 慶中華民國建國百年暨中國大陸戰略學術交流 請踴躍報名!!_0504.doc
- 慶中華民國建國百年暨中國大陸戰略學術交流 請踴躍報名!!_ATT44473.doc
- 國際關係學會第四屆學術研討會_1000609agenda.doc.rar
- s_馬英九-?.+v.s.-.pdf
- 7月6日(週三)10:30-12:30-超越帝國邊境：沖繩民族運動的形成、發展與轉型--附議程表_A..
- 級作業通知暨幫助_ATT23839.rar
- 兩岸軍事互信之契機與陰生_-pdf
- 0學年度第1學期選課相關事宜 請查照_.2.doc
- 2011-07-26 _titx@www2.tku.edu.tw_轉寄：函知100學年度第1學期選課相關事宜 請查照_.4.doc
- 2011-07-26 _titx@www2.tku.edu.tw_轉寄：函知100學年度第1學期選課相關事宜 請查照_.ATT13628.doc
- 2011-08-01 _mikina89@ndu.edu.tw_請及時將附件的資料補齊_ATT81208.doc

General Public Suffers from Malicious Emails



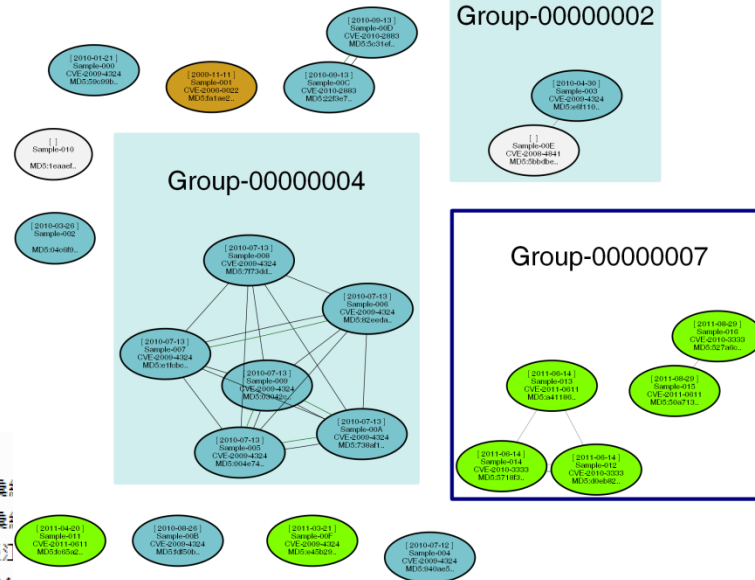
APT File Cluster Graph
Powered by Xecure Lab 2011, <http://www.xecure-lab.com>

- 2010-03-08_www71625@yahoo.com.tw_超牛B,中國第一級品帥哥的P
- 2010-04-03_yk397@yahoo.com.tw_小小S老工夜店附近辣妹(副圖)淫照
- 2010-04-18_bank.csc@inibr.chinatrust.com.tw_中國信託提醒通知函_1
- 2010-04-26_adolfo0314@yahoo.com.tw_劈腿中的真正的高手..._lnk
- 2010-04-26_service@cht.com.tw_本公司公告自99年4月起調降ADSL電
- 2010-05-05_wod1129@yahoo.com.tw_淑女也瘋狂：如何問驅最誘惑
- 2010-05-14_wod1129@yahoo.com.tw_十個方法全面“搞定”花心男
- 2010-05-17_wod1129@yahoo.com.tw_靈感都來了,悲劇啊....._rar
- 2010-05-18_wod1129@yahoo.com.tw_情侶露臉自拍,女太淫蕩了,極品
- 2010-05-19_wod1129@yahoo.com.tw_夫妻自拍,女被搞還睡得像死豬
- 2010-07-27_henry_0823@yahoo.com.tw_99年度國防淨評估論壇_99(I
- 2010-08-08_cht_ebpp@cht.com.tw_中華電信99年7月電信費用收據(國
- 2010-08-16_tsukhn07@yahoo.com.tw_黃昭順競選辦公室新聞稿 (08.16)_20100816.pdf
- 2010-08-16_tsukhn07@yahoo.com.tw_黃昭順競選辦公室新聞稿 (08.16)_20100816.pdf
- 2010-09-16_chfutsai@yahoo.com.tw_空軍學術研討會與會調查事宜_1.doc
- 2010-09-16_chfutsai@yahoo.com.tw_空軍學術研討會與會調查事宜_2.doc

- 營養健康一生_ATT27863.pps
- 當代在校大學生的性交場面_ATT15243.rar
- 淫蕩女學生_ATT61661.rar
- 電信100年5月電信費用通知單[郵件編號 101145838]_0932141701_10005_receipt_notification_w_Fw Fwd FW 2010國家地理雜誌~攝影大賽_2010~photo.pps.rar
- _星座分析：絕不可能為女友改變的男生星座_ATT25502.rar
- _處男與非處男的區別_ATT59966.rar
- 調「馬總統滿意度」；2012年總統大選」民調_P-285.pdf
- 電信100年6月電信費用通知單[郵件編號 103596889]_0932141701_10006_notification.pdf
- _Fw 男人為什麼會覺得別人老婆好_ATT17197.pdf
- 嚼蘋果核等於吃毒藥_ATT55154.pdf
- 吃飯不當致命飲食健康指標少於5條及時改_5.pdf

- 2011-07-06_ebill@ebill.skbank.com.tw_新光銀行2011年7月7日信用卡電子帳單_20117.rar
- 2011-08-04_viki.info@yahoo.com.tw_「二〇一一年臺北國際航太暨國防工業展」_2011-TAIPEI.doc
- 2011-08-26_hsatn7788@yahoo.com.tw_台灣安保協會「亞太區域安全與台灣和平」國際研討會邀請函_20110907.doc
- 2011-08-26_hsatn7788@yahoo.com.tw_台灣安保協會「亞太區域安全與台灣和平」國際研討會邀請函_20110907.pdf

Government Suffers from Malicious Emails



- 2010-03-06_press02@mofa.gov.tw_ATT64535.pdf
- 2010-03-31_beneco.taipei@webmail.gov.tw_每日網情彙!
- 2010-03-31_beneco.taipei@webmail.gov.tw_每日網情彙!
- 2010-04-03_edward46@mail.moe.gov.tw_敬邀參加「淡江
- 2010-04-06_jchiang@webmail.gov.tw_小組會議報告9904
- 2010-05-01_pishin@ey.gov.tw_請問馬總統博士陛下_ATT1
- 2010-07-11_chengkunm@gsn.gov.tw_美國聯邦調查局公佈
- 2010-07-12_ljwi@nsb.gov.tw_美俄「間諜門」_ATT54496.1
- 2010-07-18_lennkuo@mail.gio.gov.tw_由兩岸的「經濟合作架構協議」解竹田由良易的演說_-.pdf
- 2010-07-19_rensianw@mac.gov.tw_ECFA文本的特色與意含_ECFA.pdf
- 2010-07-26_mishus@gsn.gov.tw_電腦科技對空軍航電系統之衝擊_ATT21407.pdf
- 2010-07-28_anws1@ms1.anws.gov.tw_特寫臺北人氣美食TOP5_TOP5.pdf
- 2010-07-28_ljw@gsn.gov.tw_990729網情彙編_-990729.pdf
- 2010-08-25_dtmcs55@ms1.gsn.gov.tw_小心! 間諜插座就在你身邊! _ATT74891.pdf
- 2010-10-10_mofa.gov.tw_2010年10月大陸與兩岸情勢簡報_010151428148.pdf
- 2010-10-10_mofa.gov.tw_2010年10月大陸與兩岸情勢簡報_0101514282767.pdf
- 2010-10-10_mofa.gov.tw_行政院施行調查局組織法_ATT13562.doc
- 2010-10-10_mofa.gov.tw_總統、立委擬二合一之聲明_138.pdf
- 2010-10-10_mofa.gov.tw_彙整結果 請參考_100.3.rar
- 2010-10-10_mofa.gov.tw_對馬總統103年實施十二年國教誠意的質疑_.rar
- 2010-10-10_mofa.gov.tw_戰略所邀您參加 - 第七屆紀念鈕先鍾老師戰略學術研討會_-0407.rar
- 2010-10-10_mofa.gov.tw_中選會對第8屆立法委員及第13任總統將合併選舉之說明_813.doc
- 2011-04-19_nychui@cec.gov.tw_中選會對第8屆立法委員及第13任總統將合併選舉之說明_813.pdf
- 2011-06-26_rdec@rdec.gov.tw_行政院研考會近三年施政績效總說明_ATT78460.doc
- 2011-06-26_taiwanhealth@doh.gov.tw_行政院衛生署國民健康局公益郵件_ATT29433.pdf
- 2011-07-03_tobacco@bhp.doh.gov.tw_男人日常生活中的宜與忌_ATT22223.doc
- 2011-08-29_jazn2085@email.cib.gov.tw_少年仔火氣指數診斷新招_0901.pdf
- 2011-08-29_ynlin@oop.gov.tw_附件_ATT59379.doc

APT File Cluster Graph

Powered by Xecure Lab 2011, <http://www.xecure-lab.com>

Malicious Document Bites Taiwan Continuously

2011-05-03_kc168.wang@msa.hinet.net_穆斯林晉僑土葬_美火速海葬實拉登遭押解_ATT09743.doc
2011-05-04_titx@www2.tku.edu.tw_戰略所【第一屆中華民國建國百年暨中國大陸戰略學術交流】請踴躍報名!!_0504.doc
2011-05-04_titx@www2.tku.edu.tw_戰略所【第一屆中華民國建國百年暨中國大陸戰略學術交流】請踴躍報名!!_ATT44473.doc
2011-05-13_sid911030@hotmail.com_fw_保持瓶最好一次喝完...(health_tips)_ATT19017.rar
2011-05-16_cht_ebpp@cht.com.tw_中華電信100年5月電信費用通知單(郵件編號 101145838)_0932141701_10005_receipt_notification.p...
2011-05-17_c2p2lin@gmail.com_拙作一篇,請不吝指正_US Accommodation School from Budding to Rising.rar
2011-05-18_kenwclai999@yahoo.com.tw_fw_Fwd FW 2010國家地理雜誌~攝影大賽_2010~photo.pps.rar
2011-05-18_titx@www2.tku.edu.tw_2011年中華民國國際關係學會第四屆學術研討會_1000609agenda.doc
2011-05-18_vincent_lee1977@yahoo.com_中國對臺政策:演變、特徵、與變數_taiwan- resoucod.scr.txt
2011-06-02_BosKucing@gmail.com_快速致富系統'speedwealth'講座_ATT67265.doc
2011-06-13_adolfo0314@yahoo.com.tw_星座分析:絕不可能為女友改變的男生星座_ATT25502.rar
2011-06-15_ewy909@ms15.hinet.net_極品大陸女模,女神玉體!(限)_ajkh-01.jpg
2011-06-15_ewy909@ms15.hinet.net_極品大陸女模,女神玉體!(限)_ajkh-03.jpg
2011-06-15_ewy909@ms15.hinet.net_極品大陸女模,女神玉體!(限)_ATT06178.rar
2011-06-18_www71625@yahoo.com.tw_處男與非處男的區別_ATT59966.rar
2011-06-20_8bit@ufo.org.tw_51區間諜飛機,完好無損_0.pdf
2011-06-21_ttplaying@hotmail.com_fw_癌的最新發現!早點感覺_ATT34094.rar
2011-06-22_cmwang@cs.nchu.edu.tw_蔡英文+v.s.馬英九-?-v.s.-.pdf
2011-06-22_dcyang@dppnff.tw_20110622中國暨兩岸情勢日誌_20110622.doc
2011-06-22_dcyang@dppnff.tw_20110623中國暨兩岸情勢日誌_20110623.doc
2011-06-22_joechen8629@gmail.com_歡迎參加國立臺灣科學教育館大品科學講座「身體知多少」系列_ATT47042.doc
2011-06-22_johnli@nfp.org.tw_為台灣守住每一吋良田_ATT17788.pdf
2011-06-23_maow.sheng@msa.hinet.net_資生堂會員05月份得獎公布名單及資訊_05.pdf
2011-06-23_shuerlin@taiwanthinktank.org_國際油價疲軟造成的影響_ATT33684.pdf
2011-06-24_gysrc@cwgv.com.tw_遠見民調「馬總統滿意度;2012年總統大選」民調_P-285.pdf
2011-06-26_cht_ebpp@cht.com.tw_中華電信100年6月電信費用通知單(郵件編號 103596889)_0932141701_10006_notification.pdf
2011-06-26_qingsi_w85@yahoo.com.tw_fw_男人為什麼會覺得別人老婆好_ATT71797.pdf
2011-06-26_rdec@rdec.gov.tw_行政院研考會近三年施政績效總說明_ATT78460.doc
2011-06-26_taiwanhealth@doh.gov.tw_行政院衛生署國民健康局公益郵件_ATT29433.pdf
2011-06-27_arise_8546@yahoo.com.tw_順平果核等於吃毒蒜_ATT55154.pdf
2011-06-27_jingciang.su@gmail.com_fw_兩岸軍事互信機制的虛與實,請參閱_ATT53252.pdf
2011-06-27_liqiqi93@yahoo.com.tw_fw_吃飯不當致命飲食健康指標少於5條及修改_5.pdf
2011-06-27_sandy.shen@msa.hinet.net_網路倒蔡評論 請踴躍參_ATT94950.doc
2011-06-30_nan.yang@msa.hinet.net_卡內基國際和平基金會「面向2012年兩岸關係的挑戰」國際學術研討會_2012.pdf
2011-07-03_tobacco@bhp.doh.gov.tw_男人日常生活中的宜與忌_ATT22223.doc
2011-07-04_dingyu.wang@msa.hinet.net_國親合作去與從_ATT00596.doc
2011-07-04_gardner_keith@yahoo.com_台灣某組合成員被斷斷斷斷 暖昧隱私密照遭外洩_pic.rar
2011-07-04_gardner_keith@yahoo.com_共軍訓練遊藝 美為假想敵_ATT52694.rar
2011-07-04_info@ms1.hinet.net_HiNet MS1~MS59 郵件系統升級作業通知_hinet.pdf
2011-07-04_mayho@nccu.edu.tw_【亞太論壇】07月6日(週三)10:30-12:30--超越帝國邊境:沖繩民族運動的形成、發展與轉型--附議程表_A...

Confidential & Proprietary, Xecure Lab

om.tw... 修改日期: 2011/9/3 下午 02:12 建立日期: 2011/9/3 下午 02:12
大小: 1.02 MB

2011-07-06_ebill@ebill.skbank.com.tw_新光銀行2011年7月7日信用卡電子帳單_20117.rar
2011-07-06_hauyauchen@yahoo.com_同學會8_15-21花蓮之旅_201108.doc
2011-07-06_ms.chou@msa.hinet.net_fw_民進黨李安影響民調_ATT29299.pdf
2011-07-10_nature.trail@msa.hinet.net_fw_媒體總統辯論會 透視馬蔡優劣_ATT62461.doc
2011-07-10_york_chen@hotmail.com_中國海軍軍力擴張與東亞安全情勢_ATT30145.rar
2011-07-12_ej616.liu@msa.hinet.net_夏季防範十大誤區_ATT05498.doc
2011-07-13_wendy@nccu.edu.tw_fw_郵件系統升級作業通知暨幫助_ATT23839.rar
2011-07-14_andy.shu@msa.hinet.net_美國防部發布首份《網絡空間行動戰略》_ATT16661.doc
2011-07-14_jun.chun@msa.hinet.net_fw_測測你吃進去的塑化劑有什麼影響_ATT84548.doc
2011-07-15_hungchenling@yahoo.com_0715(定稿)_07150.doc
2011-07-17_abs.taiwan100@gmail.com_敬邀 全球視野下的東亞民主與台灣經驗國際學術研討會(台大政治系承辦)_agenda_democracy in e...
2011-07-17_ltc88888@ms2.hinet.net_壓力自我測試表 請保持健康_ATT61233.doc
2011-07-20_abs.taiwan100@gmail.com_Democracy in East Asia and Taiwan in Global Perspective_agenda_democracy in east asia and t...
2011-07-20_titx@www2.tku.edu.tw_fw_南海問題-兩岸軍事互信之契機與衍生-.pdf
2011-07-24_shtin99.john@msa.hinet.net_fw_高雄安全注意事項_ATT10433.doc
2011-07-26_titx@www2.tku.edu.tw_轉寄: 函知100學年度第1學期選課相關事宜, 請 查照, _2.doc
2011-07-26_titx@www2.tku.edu.tw_轉寄: 函知100學年度第1學期選課相關事宜, 請 查照, _4.doc
2011-07-26_titx@www2.tku.edu.tw_轉寄: 函知100學年度第1學期選課相關事宜, 請 查照, _ATT13628.doc
2011-07-27_chao.wei@msa.hinet.net_通州動車脫軌事故安全警示_ATT43518.rar
2011-07-31_honto.denki@msa.hinet.net_fw_early headlines_headlines.doc
2011-08-01_mikina89@ndu.edu.tw_請及時將附件的資料補齊_ATT81208.doc
2011-08-02_engkong.kh@msa.hinet.net_台灣基督長老教會2011年行事曆_20110.xls
2011-08-04_ebill@ebill.skbank.com.tw_台灣大哥大100年07月份電子帳單寄送函_10007-9824584706114A022645-receipt.pdf.rar
2011-08-04_justin.fanny@msa.hinet.net_非凡美食大探索_861-7145.xls
2011-08-04_wiki.info@yahoo.com.tw_「二〇一一年臺北國際航太暨國防工業展」_2011--TAIPEI.doc
2011-08-08_Council@us-taiwan.org_Agenda for US-Taiwan Defense Industry Conference 2011_Agenda - US-Taiwan Defense Industry C...
2011-08-08_jojobox@ms21.hinet.net_爸爸節快樂!_ATT50833.rar
2011-08-24_thoughts168@gmail.co_國防部整合評估室誠摯邀請各位貴賓出席8_29歡迎酒會及8_31晚宴_ATT10933.rar
2011-08-26_hsatn7788@yahoo.com.tw_台灣安保協會「亞太區域安全與台海和平」國際研討會邀 請 函_20110907.doc



Top 3 Academic Institutions being Targeted in Taiwan: Sinica, NCCU, TKU

 2010-05-07 _lsf@gate.sinica.edu.tw_201004_遠見民調中心_台灣民眾政黨傾向追蹤分析_GVSRP_PID_201004_C.pdf
 2010-10-22 _tsa@gate.sinica.edu.tw_東海大學社會學系：閔丙甲教授演講_ATT25721.pdf
 2010-11-12 _tsa@gate.sinica.edu.tw_Fw 轉寄 政府組織再造 心理健康司的發展_.pdf
 2011-03-08 _ytl@gate.sinica.edu.tw_「《歐美研究》四十週年」座談會邀請函_ATT19907.doc

 2011-07-04 _mayho@nccu.edu.tw_【亞太論壇】07月6日(週三)10 30-12 30--超越帝國邊境：沖繩民族運動的
 2010-07-07 _ykkao@nccu.edu.tw_關於中共領導人&_35843;查研究_.pdf
 2010-08-23 _tasims9@nccu.edu.tw_第二屆「半總統制與民主」學術研討會_ATT72404.pdf
 2011-07-13 _wendy@nccu.edu.tw_FW 郵件系統升級作業通知暨幫助_ATT23839.rar
 2010-11-04 _making@nccu.edu.tw_修正版如附件_ATT69914.pdf
 2010-11-08 _kh8877@nccu.edu.tw_Fw 991每位老師TA及CA補助費用（選課更正後）_99(1)TA-RA -.rar
 2010-06-08 _iirj@nccu.edu.tw_天安艦後的朝鮮半島新局勢_ATT77316.pdf
 2010-07-11 _iirj@nccu.edu.tw_雙週報 1579期_ATT50892.pdf
 2010-05-03 _zhonggonv@nccu.edu.tw_2010 年中共年報_2010 .doc
 2010-05-03 _zhonggonv@nccu.edu.tw_2010 年中共年報_2010 .pdf
 2010-10-06 _fen6604@nccu.edu.tw_美國公布共軍軍力報告的重大意義_ATT93278.pdf

Top 3 Academic Institutions being Targeted in Taiwan: Sinica, NCCU, TKU

-  2010-03-24 _h670928@ndu.edu.tw_2010第十八屆國防管理學術暨實務研討會_ATT43728.pdf
-  2011-06-22 _cmwang@cs.nchu.edu.tw_蔡英文 + v.s. 馬英九 - ?_+v.s. -.pdf
-  2010-10-27 _titx@www2.tku.edu.tw_Fw 11_10研討會議程_Document.pdf
-  2010-10-27 _tivx@tku.edu.tw_11_10研討會議程_Document.pdf
-  2011-02-24 _titx@www2.tku.edu.tw_[重要]敬邀參與本校2011年「春之饗宴」活動_2011.doc
-  2011-07-26 _titx@www2.tku.edu.tw_轉寄：函知100學年度第1學期選課相關事宜，請 查照。_4 .doc
-  2011-05-04 _titx@www2.tku.edu.tw_戰略所【第一屆中華民國建國百年暨中國大陸戰略學術交流】請踴躍報名!!
-  2011-05-04 _titx@www2.tku.edu.tw_戰略所【第一屆中華民國建國百年暨中國大陸戰略學術交流】請踴躍報名!!
-  2011-05-18 _titx@www2.tku.edu.tw_2011年中華民國國際關係學會第四屆學術研討會_1000609agendadoc.rar
-  2011-07-20 _titx@www2.tku.edu.tw_Fw 南海問題-兩岸軍事互信之契機龔隆生_-.pdf
-  2011-07-26 _titx@www2.tku.edu.tw_轉寄：函知100學年度第1學期選課相關事宜，請 查照。_2 .doc
-  2011-07-26 _titx@www2.tku.edu.tw_轉寄：函知100學年度第1學期選課相關事宜，請 查照。_ATT13628.doc
-  2010-03-08 _titx@oa.tku.edu.tw_敬邀參加兩岸關係研討會_.pdf
-  2010-12-17 _126251@mail.tku.edu.tw_敬祝大家聖誕新年快樂_倂.doc
-  2011-04-18 _shkang@nfu.edu.tw_初稿已完成_ATT38713.rar
-  2010-10-22 _tsa@gate.sinica.edu.tw_東海大學社會學系：閔丙甲教授演講_ATT25721.pdf
-  2010-07-07 _ykkao@nccu.edu.tw_關於中共領導人&_35843;查研究_.pdf
-  2010-08-23 _tasims9@nccu.edu.tw_第二屆「半總統制與民主」學術研討會_ATT72404.pdf

Exploit Hiding in Legitimate Content

CVE Number	Attachment (rename as Date, Sender, Email Title)
CVE-2009-4324	2010-05-07_lsf@gate.sinica.edu.tw_201004_遠見民調中心_台灣民眾政黨傾向追蹤分析_GVSRP_PID_201004_C.pdf
CVE-2009-4324	2010-10-22_tsa@gate.sinica.edu.tw_東海大學社會學系：閔丙甲教授演講_ATT25721.pdf
CVE-2010-2883	2010-11-12_tsa@gate.sinica.edu.tw_Fw 轉寄 政府組織再造 心理健康司的發展_.pdf
CVE-2010-2883	2010-10-06_fen6604@nccu.edu.tw_美國公布共軍軍力報告的重大意義_ATT93278.pdf
CVE-2006-2492	2011-03-08_ytl@gate.sinica.edu.tw_「《歐美研究》四十週年」座談會邀請函_ATT19907.doc
CVE-2009-4324	2010-05-03_zhonggonv@nccu.edu.tw_2010 年中共年報_2010 .pdf
CVE-2009-4324	2010-06-08_iirj@nccu.edu.tw_天安艦後的朝鮮半島新局勢_ATT77316.pdf
CVE-2009-4324	2010-07-11_iirj@nccu.edu.tw_雙週報 1579期_ATT50892.pdf
CVE-2009-4324	2010-08-23_tasims9@nccu.edu.tw_第二屆「半總統制與民主」學術研討會_ATT72404.pdf
CVE-2010-3333	2011-07-04_mayho@nccu.edu.tw_【亞太論壇】07月6日(週三)10 30-12 30--超越帝國邊境：沖繩民族運動的形成、發展與轉型--附議程表_ATT81166.doc

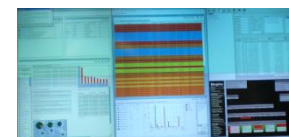
Confidential & Proprietary, Xecure Lab



Cyber Espionage Loves APT

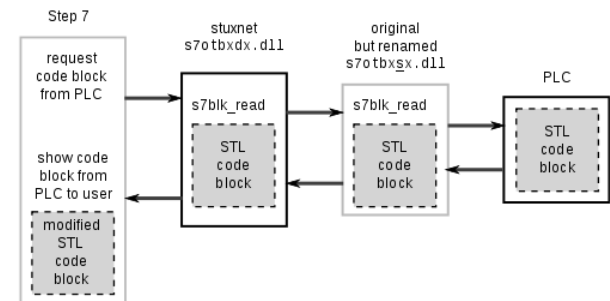
Advanced Persistent Threat

- * Get ready for a war without smoke
- * Winners are ahead of the game
 - * Know exactly where to escalate and be **advanced**
- * Winners last longer
 - * Know exactly how to stay low-profile and **persistent**
- * Victims all failed to **"know the enemy, know yourself"**



SCADA Systems Are Targeted

- * 2010.7.14 Stuxnet
 - * Planned: Stole certificates from two Taiwan high-techs
 - * Organized: Shall have 10 people six months to write
 - * Advanced: Use several vulnerabilities, including four zero-day exploits
 - * Persistent: It waits until it finds Siemens SIMATIC WinCC/Step 7 controller software



1% Click-through Rate Kills 99% Enterprise

- * 2010.1.14 Operation Aurora (Hydraeq trojan) had compromised Google, Adobe, and more than several dozens of large enterprises

- * JavaScript code exploited a 0-day in IE 6.0 (CVE-2010-0249)

Confidential & Proprietary, Xecure Lab

[illegible]

Transparency: Operation Aurora

Google and Adobe garnered praise from many information security professionals recently after admitting their systems had been compromised.

Such transparency is commendable because it could prompt other companies to become more secure, said Patrik Runald, senior manager of security research at web security firm Websense. The fact that Google admitted it was a target, was a significant step, Runald said.

"If nothing else, I think it will help going forward because people will look at their own security and look at what they can do to protect themselves," he said.

The attack, dubbed "Operation Aurora," leveraged a

previously unknown vulnerability in Internet Explorer to compromise systems at Google, Adobe and more than 30 other large companies. Google disclosed the hack in a Jan. 12 blog post. That same day, Adobe came forward and said it was one of the victimized companies.

"Transparency for our customers and partners was a key factor in Adobe's decision to go public with the information," said Wiebke Lips, a spokesperson at Adobe. "This incident demonstrates the increased sophistication in today's malware design and attack strategies. It also serves as a reminder of the importance of multiple layers of security and the need to follow security best practices."

Providing information about attacks can also help security vendors develop better products, said Chris Wysopal, CTO of application security firm Veracode.

"I'm all for as much transparency as possible," Wyso-pal said. "When companies learn details and fix their own network, everyone else can benefit from that knowledge too."

47.3%
of targeted attacks
in 2009 were made
using the PDF file
format

Source: F-Secure

```

00 00 00 00 00 00 F0 3F 00 00 00 00 00 00 20 40 .....?.....@
00 01 00 46 75 3D A7 3F 04 8B 0A 3F 15 EF C3 3E ...Fu=???...>
F3 04 35 3F 00 00 00 00 00 00 00 00 00 00 00 00 ..5?.....
65 2B 30 30 30 00 00 00 00 00 00 00 C0 7E 01 50 41 e+000.....~.PA
00 00 00 00 FF FF 47 41 49 73 50 72 6F 63 65 73 .....GRAIsProces
73 6F 72 46 65 61 74 75 72 65 50 72 65 73 65 6E sorFeaturePresen
74 00 00 00 4B 45 52 4E 45 4C 33 32 00 00 00 00 t...KERNEL32...
31 23 51 4E 41 4E 00 00 31 23 49 4E 46 00 00 00 1#QNAN...1#INF...
31 23 49 4E 44 00 00 00 31 23 53 4E 41 4E 00 00 1#IND...1#SNAN...
52 53 44 53 91 82 FE 94 29 AB E5 42 A6 53 10 A8 RSDS....).B.S...
D2 04 69 98 10 00 00 00 66 3A 5C 41 75 72 6F 72 ...i.....f:\Auror
61 5F 53 72 63 5C 41 75 72 6F 72 61 56 4E 43 5C a_Src\Aurora\WNC\
41 76 63 5C 52 65 6C 65 61 73 65 5C 41 56 43 2E Avc\Release\AVC.
70 64 62 00 94 4D 03 10 00 00 00 00 00 00 00 00 pdb..M.....
FF FF FF FF 00 00 00 00 00 00 00 00 54 21 03 10 .....T!...
00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 .....

```

"Stepping Stone" for Further, Deeper Attack

- * 2011.3.18 RSA SecurID got compromised due to staffs lured by malicious spreadsheet named "2011 Recruitment plan.xls" that had Adobe Flash 0-day exploit (CVE-2011-0609)

Open Letter to RSA SecurID Customers



Arthur W. Coviello, Jr.

To Our Customers:

On March 17, 2011, RSA publicly disclosed that it had detected a very sophisticated cyber attack on its systems, and that certain information related to the RSA SecurID® product had been extracted. We immediately published best practices and our prioritized remediation steps, and proactively reached out to thousands of customers to help them implement those steps. We remain convinced that customers who implement these steps can be confident in their continued security, and customers in all industries have given us positive feedback on our remediation steps.

Certain characteristics of the attack on RSA indicated that the perpetrator's most likely motive was to obtain an element of security information that



Mar 18,
2011

SECURITY

RSA SecurID Hack Shows Danger of APTs

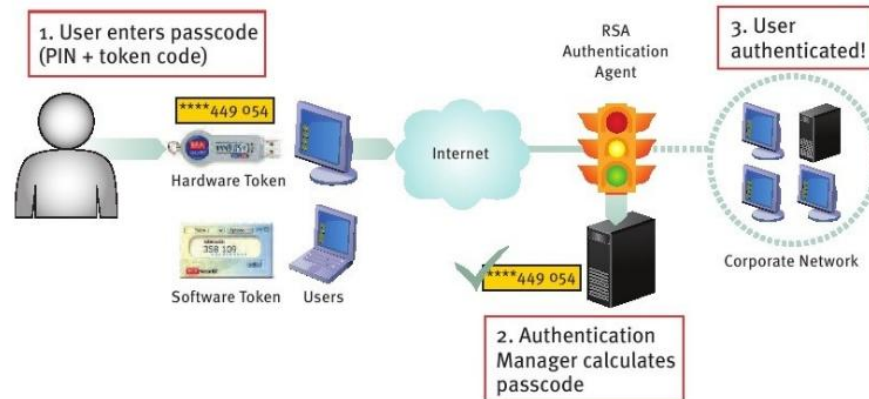
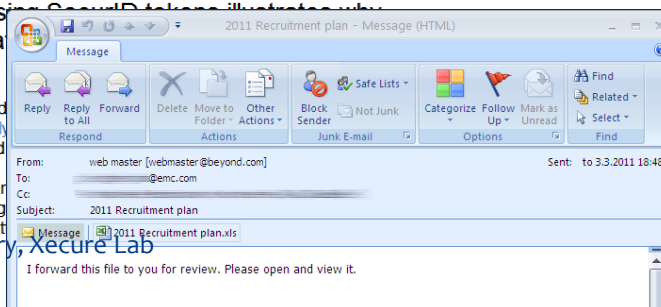
The RSA hack compromises SecurID tokens illustrating an advanced persistent threat

By Tony Bradley

Mar 18, 2011 10:10 AM

RSA revealed in an open letter posted data was stolen which could potentially network is an example of a new breed going after bigger payoffs.

RSA describes the attack as an advance involves patient, skilled, well-funded at



Defense Contractors Are the Real Targets

- * 2011.5.28~
Lockheed Martin, L-3,
Northrop Grumman all got
attacked, and stolen RSA
SecurID info were leveraged

Palisade: Cyber Security for the Utility and Energy Industry

May 30, 2011

30 May 2011 Last updated at 11:07 GMT

US defence firm Lockheed Martin hit by cyber-attack

US defence firm Lockheed Martin says it has come under a significant cyber-attack, which took place last week.

Few details were available, but Lockheed said its security team had detected the threat quickly and ensured that none of its programmes had been compromised.

The Pentagon said it is working to establish the extent of the breach.

Lockheed makes fighter jets, warships and multi-billion dollar weapons systems sold worldwide.

Lt Col April Cunningham, speaking for the US defence department, said the impact on the



Lockheed Martin makes F-16 fighter jets

Second Defense Contractor L-3 'Actively Targeted' With RSA SecurID Hacks

By Kevin Poulsen | May 31, 2011 | 4:11 pm | Categories: Hacks and Cracks

Follow @kpoulsen · 7,938 followers

EXCLUSIVE: Northrop Grumman May Have Been Hit by Cyberattack, Source Says

By Jeremy A. Kaplan
Published June 01, 2011 | FoxNews.com

Print Email Share Recommend 282 Tweet 330 +1 0



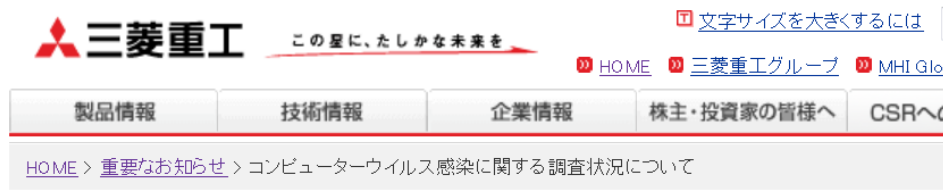
A Northrop Grumman E-2C Hawkeye 2000 surveillance and reconnaissance plane lands on a carrier.

Top military contractor Northrop Grumman Corp. may have been hit by a cyber assault, the latest in a string of alarming attacks against military suppliers, a source within the company told FoxNews.com.

Lockheed Martin said its network had been compromised last week, and defense contractor L-3 Communications was targeted recently, as well. Both intrusions involved the use of remote-access security tokens, experts say.



Mitsubishi Heavy Industry



コンピューターウイルス感染に関する調査状況について

8月中旬にウイルス感染の可能性が判明したことを受け、ただちにウイルス駆除などの被害拡大防止と監視するとともに、外部の専門家と共同で詳細な調査及び必要な対応を進めております。現時点までの調査では、社外へのデータ流出は確認されておきませんが、今回のサイバー攻撃の規模・悪質性に鑑み、当社は本事実を提出しました。

今後とも引き続き調査を進め、警察の捜査に全面的に協力してまいります。

また、当社は従来から自社の製品及び技術の重要性を認識し、高レベルの情報セキュリティを維持すべく、この事実を重く受け止め、さらなるセキュリティ強化に取り組んでまいります。

[HOME](#) > [重要なお知らせ](#) > 本日の一部報道について



2011年9月19日

三菱重工業株式会社

本日の一部報道について

本日、当社のコンピューターがウイルスに感染しているとの一部報道がありました。

8月中旬にウイルス感染の可能性が判明し、その後ウイルスの特性により情報漏えいの危険性も判明したことを受け、その旨を警察当局に報告、相談するとともに、以後、外部の専門家と共同で調査、対応を進めております。

現時点ではウイルス感染による被害拡大は止まったものと考えております。

また過去に社内一部のコンピューターのシステム情報(ネットワークアドレス等)が流出した可能性があることは判明しているものの、当社の製品や技術に関する情報の社外へのデータ流出は現在確認されておきません。

これまでウイルス駆除などの被害拡大防止策を講じておりますが、今後とも引き続き調査を進め、対策強化をはかってまいります。

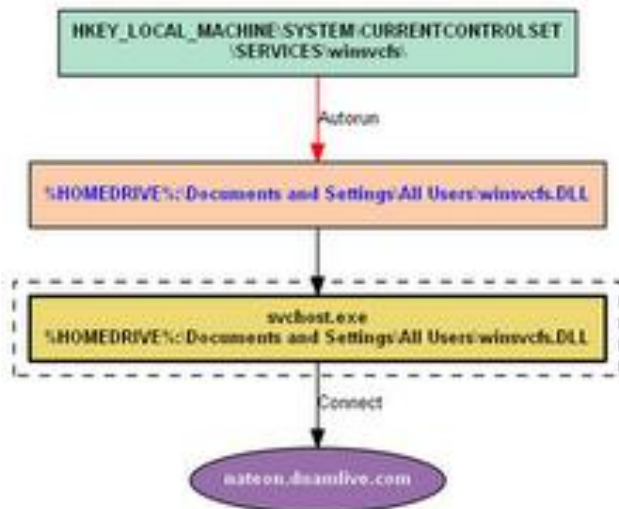
Taiwan Zombies are Abused to Infect Korean Users

- * Attackers love Personally Identifiable Information (PII)
- * 2011.7 SK Communication got hacked
 - * 35 million PII (Korea's population is about 49 million)
- * The malware that got SK Communication compromised was hosted in a compromised server in Taiwan for a during of 68.2 hours (2011-07-28 22:50:03 to 2011-07-31 19:02:19)

Date ↑↓	Closed ↑↓	hours	contributor ↑↓	virusname ↑↓	URL ↑↓
2011-07-28 22:50:03	2011-07-31 19:02:19	68.2	sub14	22/41 (53.7%) TR/ATRAPS.Gen 68	http://www.h.com.tw/act/nateon.s
2011-07-28 18:48:15	2011-07-29 00:34:21	5.8	sub8	HEUR:Trojan.Win32.Generic	http://www.h.com.tw/act/

Find Out the Enemy in the Dark

- * Found C&C and botherder



Gu...ing (w...a6@gmail.com)
+8...0128
...29
No...ad
Fu...0002
...

Malware Analysis Report

Time 2011-07-29 17:30:25
Duration 63 Seconds
Engine 2.9.1

%HOMEDRIVE%\Documents and Settings\All Users\winsvcfs.DLL
(E3D8CE21BFF2DD1882DA2775E88A9935)

Malware
Family
Build Time 2010-09
Malware Type
Severity ★

Behavior • This Malware has been identified the following behavior: **DLL-Injection** (Target: svchost.exe) functions.

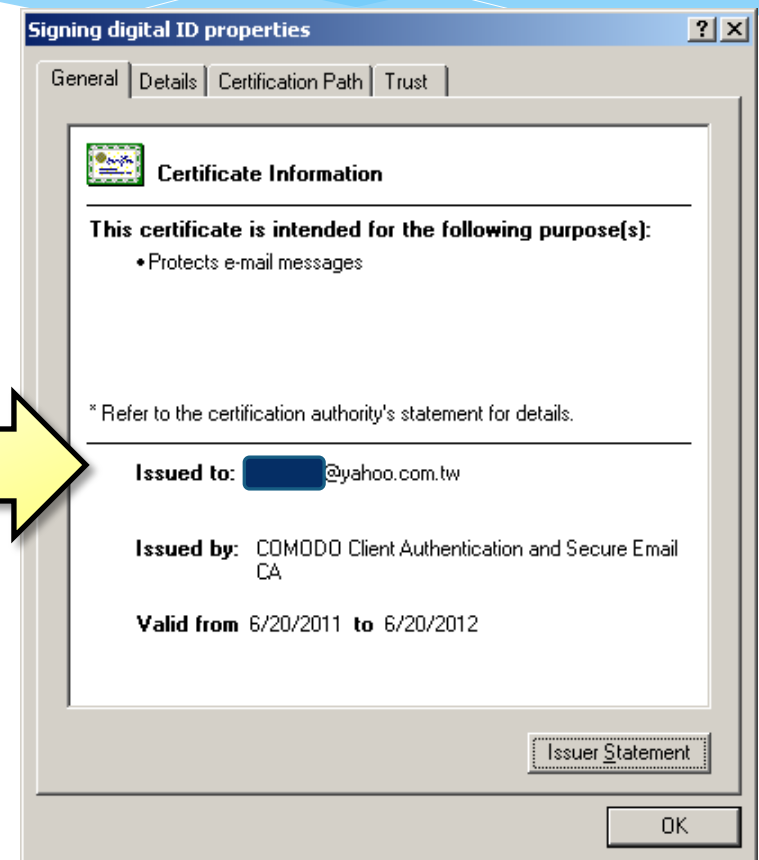
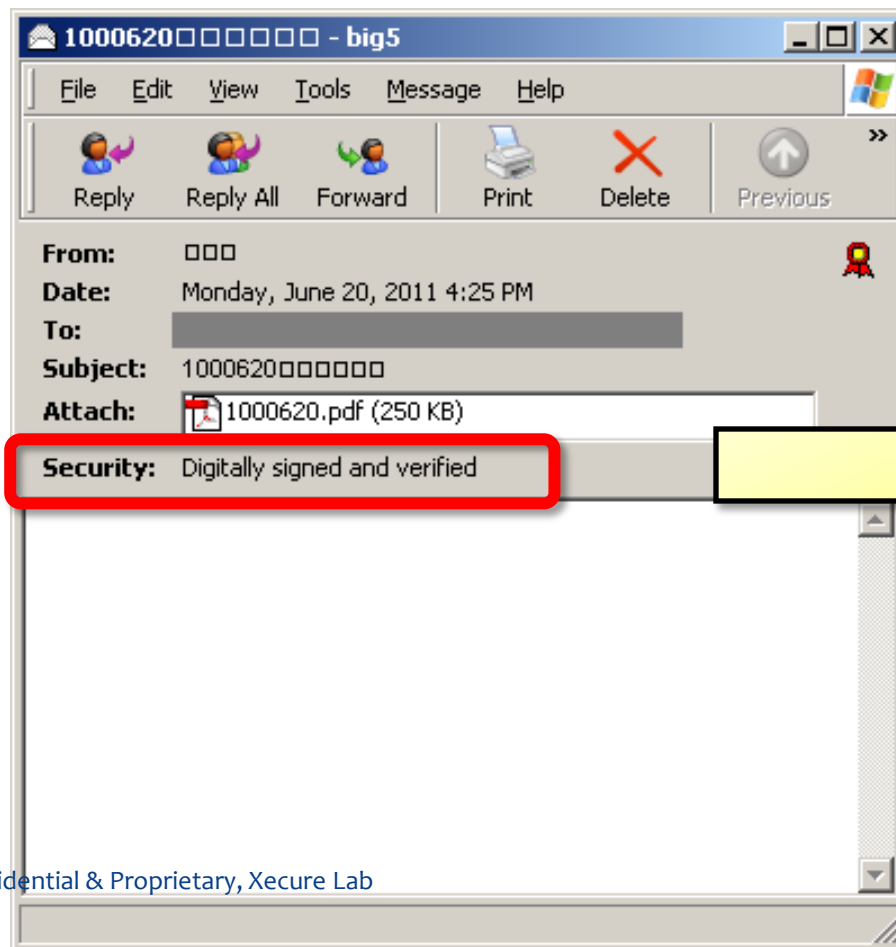
Modules • Base=10000000 Size=0008C000 svchost.exe

Files • [DLL] %HOMEDRIVE%\Documents and Settings\All Users\winsvcfs.DLL
E3D8CE21BFF2DD1882DA2775E88A9935

Autoruns • HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\winsvcfs\

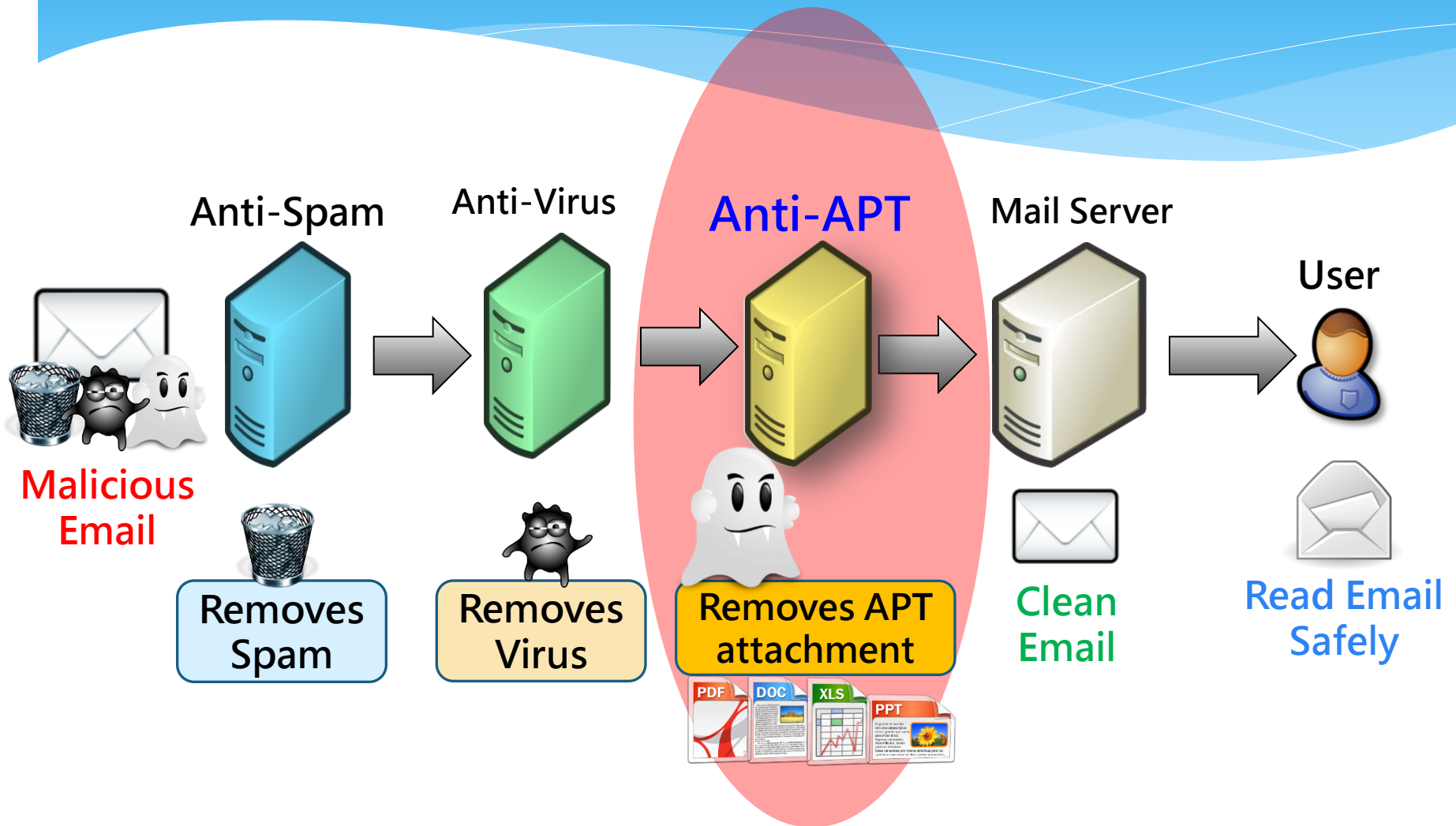
Network • nateon.d...com

Stolen Certificate Got Leveraged in Cyber Espionage



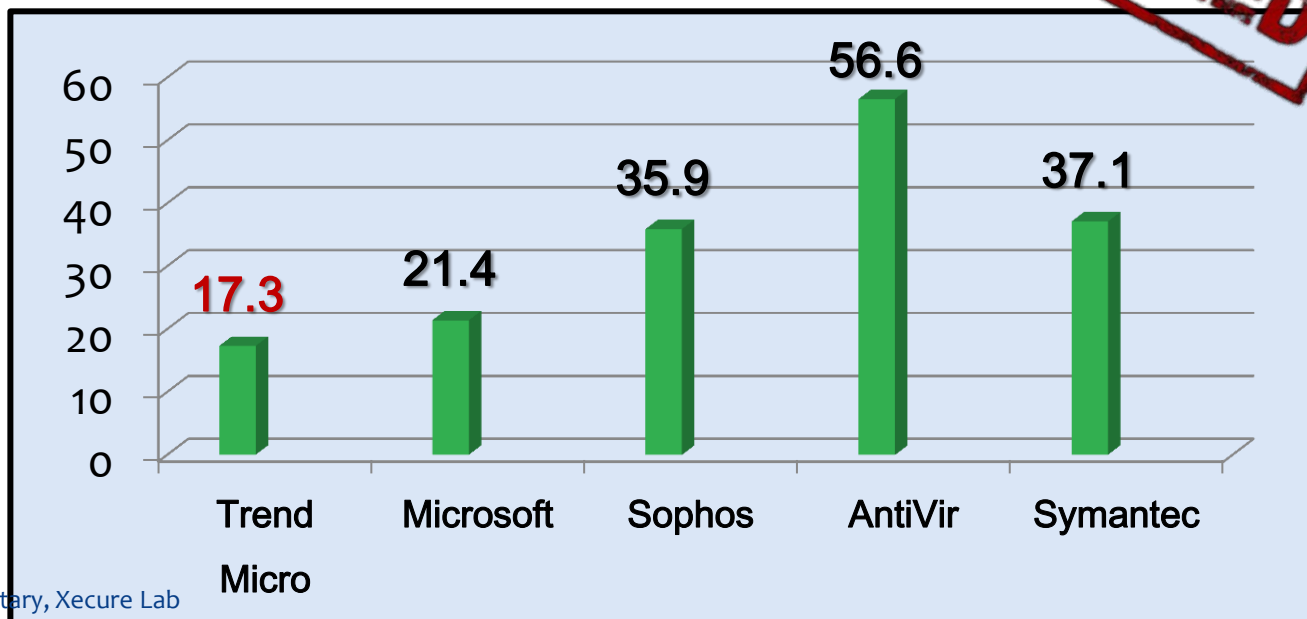
Layered Countermeasures for Cyber Espionage

Layered Protections



Anti-virus + Anti-APT = Anti-Cyber Espionage

- * Anti-virus fights virus, not APT



Cyber Combat: Act of War

THE WALL STREET JOURNAL
WSJ.com

TECHNOLOGY | MAY 31, 2011

Cyber Combat: Act of War

Pentagon Sets Stage for U.S. to Respond to Coi

By SIOBHAN GORMAN And JULIAN E. BARNES

WASHINGTON—The Pentagon has concluded that computer sabotage an act of war, a finding that for the first time opens the door for the U

“This world—cyberspace—is a world that we depend on every single day... [it] has made us more interconnected than at any time in human history.”

—President Barack Obama, May 29, 2009

INTERNATIONAL STRATEGY FOR CYBERSPACE

When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational,



Operate Effectively in Cyberspace

(OV-1: High Level Operational Concept)



Confidential & Copyright has the exclusive story of the Pentagon classifying cyber attacks by foreign nations as acts of war. Photo: THOMAS KIENZLE/AFP/Getty



Free Online Document Scanning

<http://aptdeezer.xecure-lab.com>

- * Open no document without careful inspection ;-)
- * Is it APT?
- * Who are behind it?
- * How active are they?

Xecure Deezer

aptdeezer.xecure-lab.com

Xecure-Lab APT 惡意檔案線上快篩服務

APT-DEEZER
Rapid APT Identification Service

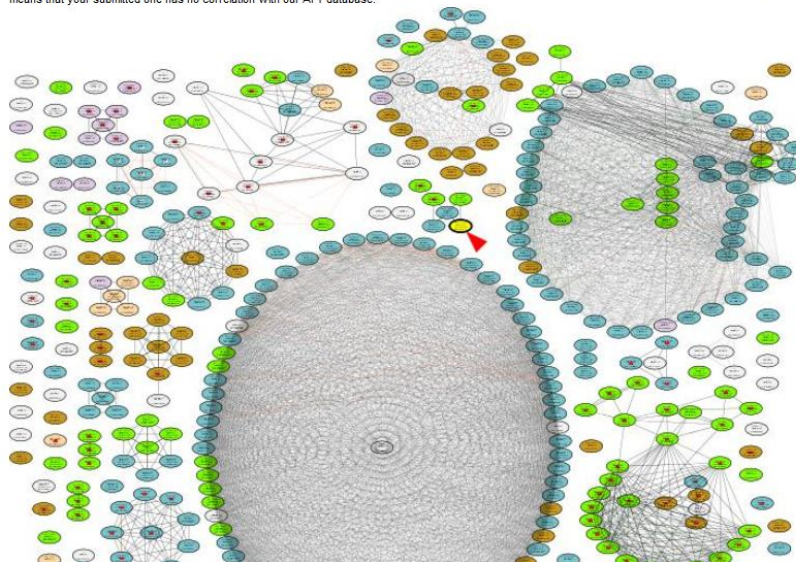
Browse... Upload

Date	Result	Group	File Name	MD5
2011/10/05	Malicious		1001Hw1.doc...	8b783a55fd7361af8f7e531...
2011/09/30	CVE-2010-3333	APT000P0	0923行程預排表更新.doc...	d1361f2691191b9f2825f62...
2011/09/30	CVE-2010-3333	APT000P0	0923行程預排表更新.doc...	d1361f2691191b9f2825f62...
2011/09/22	CVE-2011-0609		CVE-2011-0609_XLS-SW...	4bb64c1da2f73da11f331a96...
2011/09/12	CVE-2010-3333		conclusion.doc...	5dbe52f051069c7a43189eba...

Page 1 of 13

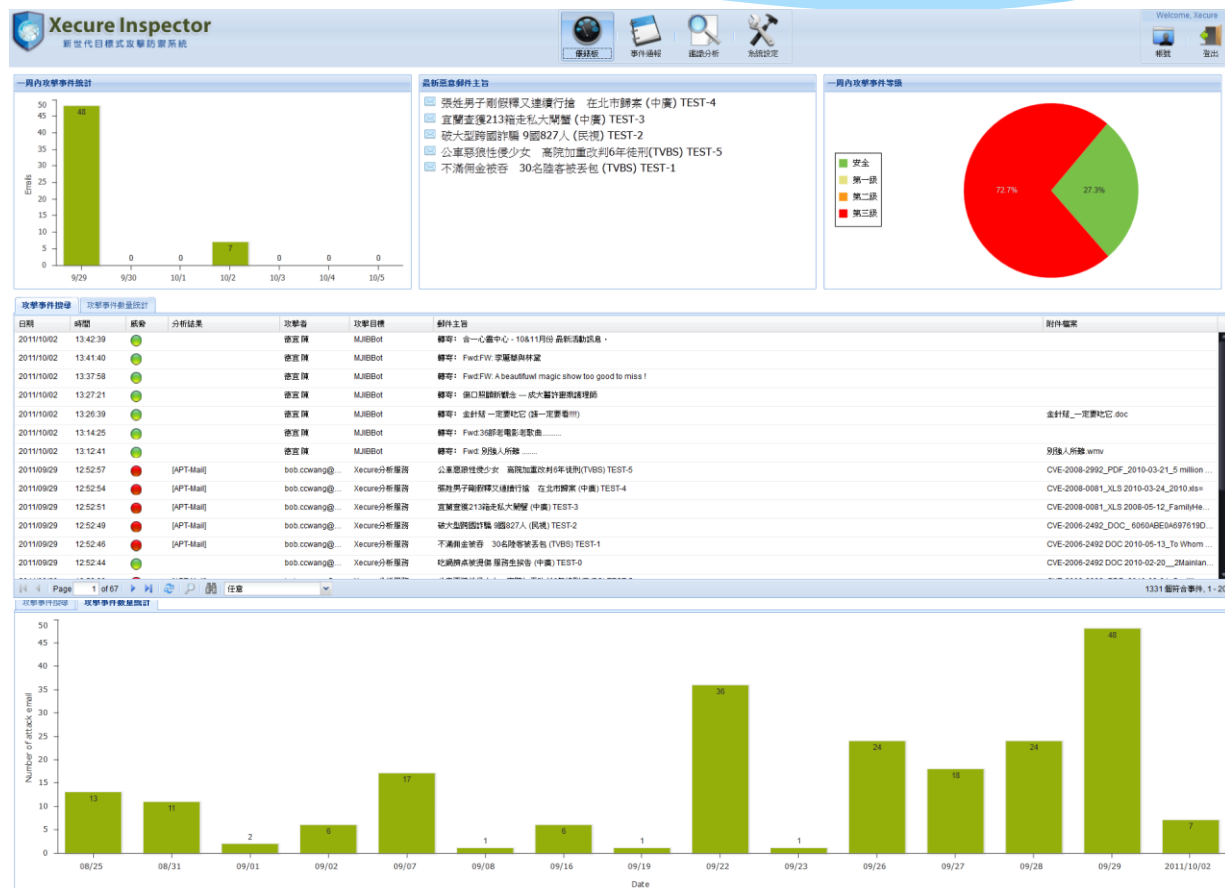
Report

Description:
You have uploaded a sample which is highlighted with yellow circle, the map showing you the sample is correlated with our APT database. If your sample falls in the group or the group is connected with lines which means that your submitted one has no correlation with our APT database.



Visualize Email Attack Frequency and Severity

- * Malicious email attack is easy and effective
- * One must overview attack trend to feel the risk
- * Then brainstorm and review defense strategy



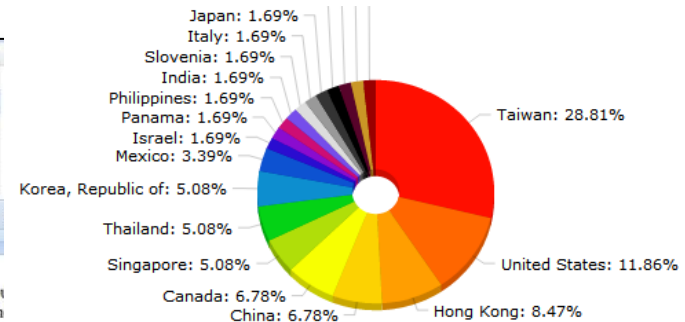
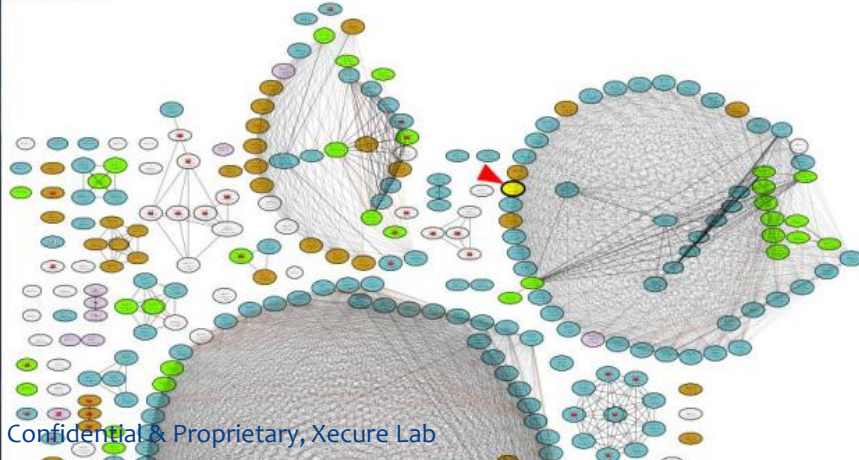
Mapping APT Taskforces with APT Victims

Date	CVE	Group ID	File Name	MD5
2011/07/12	CVE-2010-1297		CVE-2010-1297_2010-06-01_無人飛行載具之發...	8682367a5db76a4b054c963...
2011/07/12	CVE-2010-0188	APT000A0	行政院院會議程.pdf	21676f8c2d5cdfac99f833b7a...
2011/07/11	CVE-2010-3333		通訊錄.doc	7d661160bdf58e22e6e9ef0f...
2011/07/11	CVE-2010-0188		8D掌管九兆資產，個人存款不到七百萬.pdf	6b9476a9766be4770be3df4a...
2011/07/11			1000620.pdf	25df7773635a53e39569cc5a...
2011/07/09	CVE-2010-2883	APT00070	T05_CVE-2010-2883.PDF_CanType_SING.PDF	9c5cd8f4a5088acaa6c2a2dc...

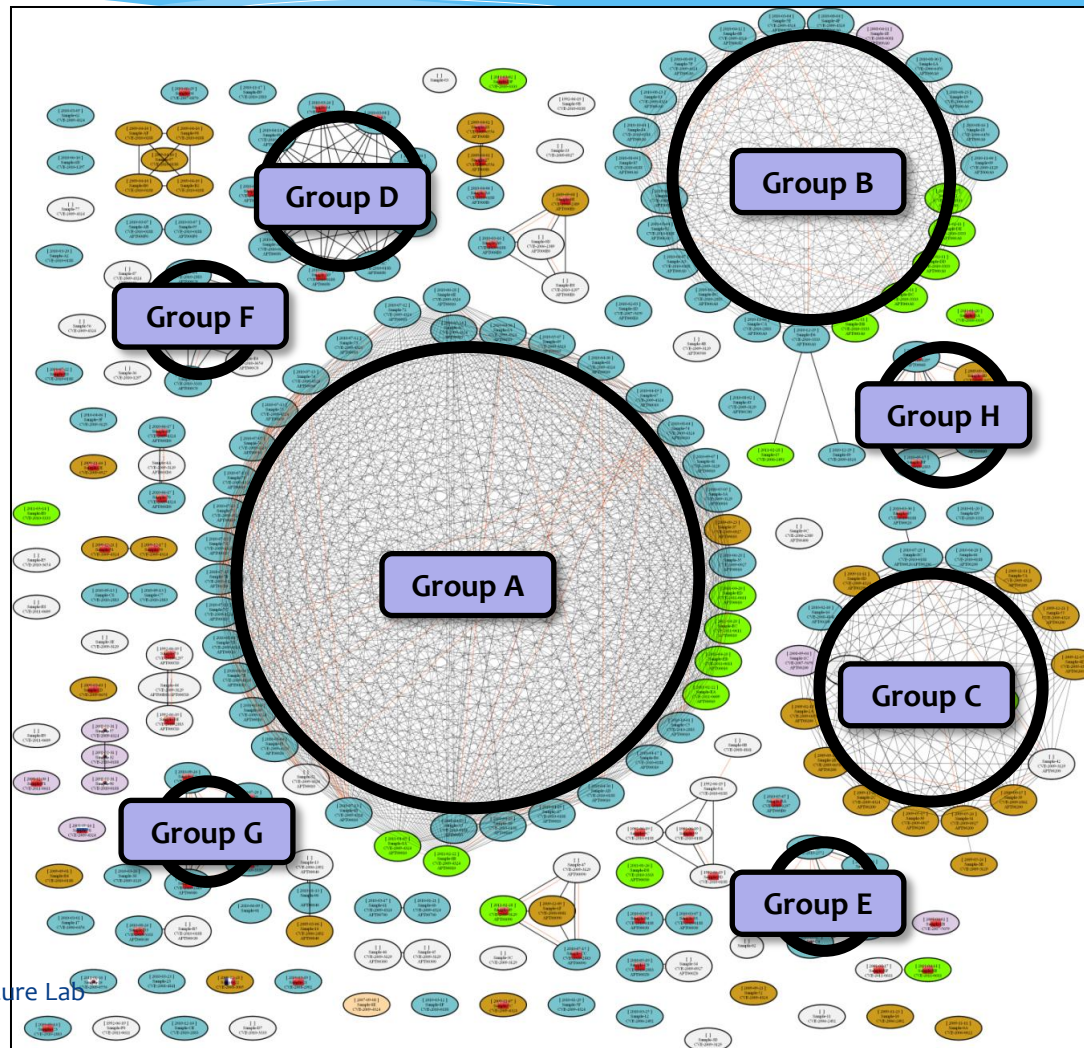
Report

Description:

You have uploaded a sample which is highlighted with yellow circle, the map showing you the sample is correlated with our APT database. If you sample falls in the group or the group is connected with lines which indicates that the sample and our APT database have correlation and relevant the contrary, if you find your sample is independent without connecting to other samples, it means that your submitted one has no correlation with APT database.



At least 8 Major Taskforces Are Behind Today's APT



2011

2010

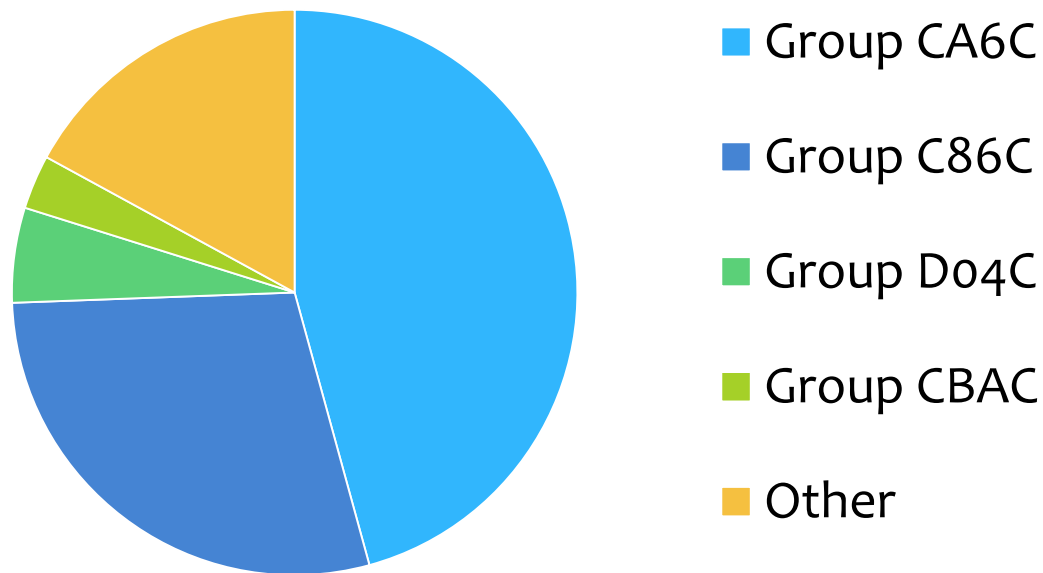
2009

2008

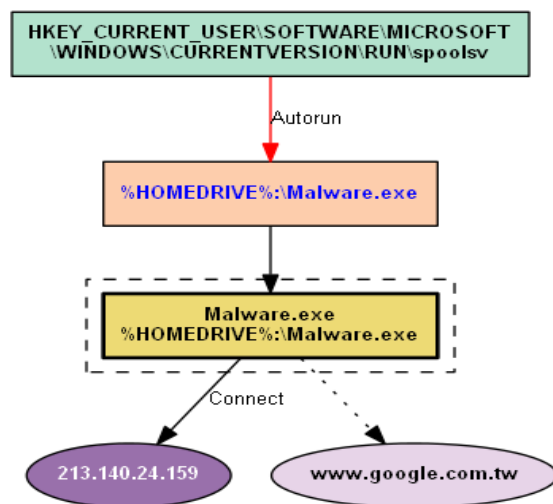
other

Cyber Espionage is Team Work

APT Document Group Graph

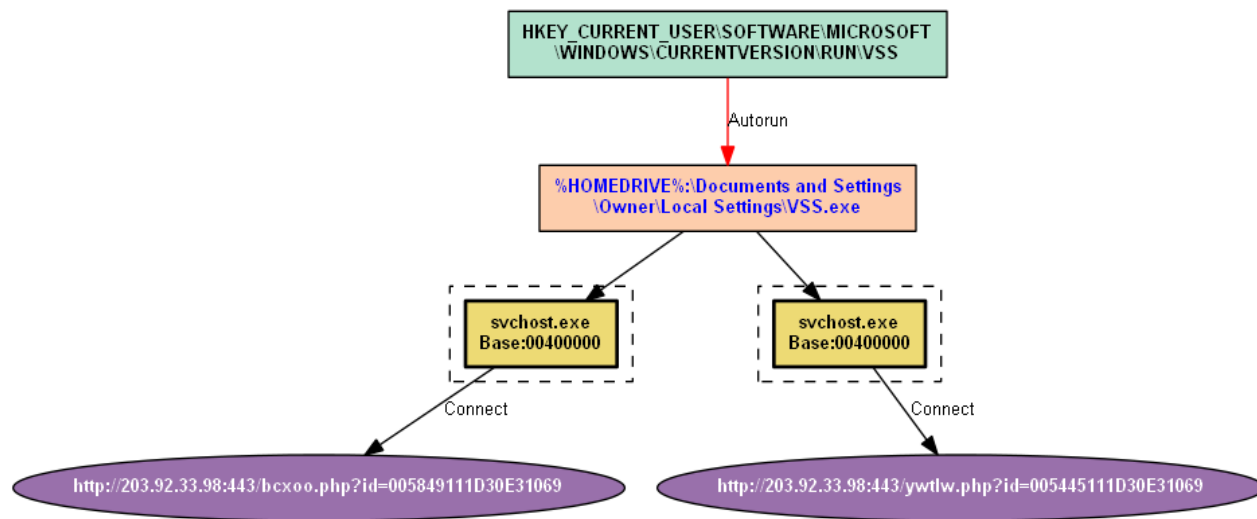


Prevent or Welcome? Command and Control...



Powered By Xecure Analyzer Engine, 2011

Confidential & Proprietary, Xecure Lab



Powered By Xecure Analyzer Engine, 2011

Popular Exploits Used in 2011 for Attacking Taiwan

CVE	Percentage
CVE-2010-3333	35%
CVE-2009-4324	30%
CVE-2011-0611	21%
CVE-2010-2883	5%
CVE-2009-0927	4%
others	10%

Conclusion

- * Cyber Espionage is team work
- * APT heavily uses emails, others use USB devices or Web drive-by downloads
- * Cyber Espionage is leveraging the 1% to destroy the 99%
- * Security must be visualized
 - * 5W1H

Thank you.

Feel free to contact me.
bensonwu@gmail.com